IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA	:	
	:	
v.	:	1:18CR492-1
	:	
TIMOTHY DONOVAN BURNS	:	FACTUAL BASIS

NOW COMES the United States of America, by and through Matthew G.T. Martin, United States Attorney for the Middle District of North Carolina, and as a factual basis under Rule 11, Fed. R. Crim. P., states the following:

Background on the Network:

The instant case involves an Internet-based, peer-to-peer (P2P) network (the "Network") that allows users to anonymously share files, chat on message boards, and access websites. In order to access the Network, a user must first download the Network software, which is free and publicly available. Anyone running this software may join and access the Network. Each computer running Network software connects directly to other computers, which are called its "peers." When installing the Network software, each user agrees to provide to the Network a portion of the storage space on the user's computer hard drive, so that files uploaded by Network users can be distributed and stored across the Network. Network users can upload files into the Network and download files from the Network.

When a user uploads a file into the Network, the software breaks the file into pieces (called "blocks") and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Network of peers.[1] The software also creates an index piece that contains a list of all of the pieces of the file and a unique key – a series of letters, numbers and special characters – that is used to download the file. In order to download a file, a Network user must have the key for the file.

When a user attempts to download a file via the Network, the Network downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Network software then requests all of the pieces of the file from the user's peers. Rather than request all of the file pieces from a single peer, requests for file pieces are divided up in roughly equal amounts among the user's peers. If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on.

This design can help law enforcement distinguish between a Network user that is the original requestor of a file, and one that is merely forwarding

[1] Because the pieces of files are encrypted, a Network user is unable to access the content of pieces that are stored on the user's computer hard drive, which are not in a readable format.

the request of another user. To prevent requests for pieces from going on indefinitely, the Network is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times. If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers. The remaining number of times a request for a piece may be forwarded is included within the request for that piece.

The Network warns its users in multiple ways that it does not guarantee anonymity. Additionally, Network software does not mask a computer's IP address — the IP addresses of each user's peers are observable to the user. The Network also acknowledges on its publicly accessible website that it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

Child Pornography on the Network:

The Network can be used to advertise and distribute images and videos of child pornography. Unlike other file sharing systems, the Network does not provide a search function for its users whereby users conduct search terms to locate files. Therefore, a user who wishes to locate and download child

pornography from the Network must identify the key associated with a particular child pornography file and then use that key to download the file.

Network users can identify those keys in a number of ways. For example, "message boards" exist on the Network that allow users to post messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: "pthc," "boy porn," "hussy," "pedomom," "kidfetish," "toddler_cp," "hurtcore," and "tor-childporn." Typical posts to those message boards contain text, keys of child pornography files that can be downloaded through the Network, and in some cases descriptions of the image or video file associated with those keys.

Network users can also obtain keys of child pornography images or videos from websites that operate within the Network. These websites can only be accessed through the Network. Some of those sites contain images of child pornography the user can view along with keys of child pornography files. It is also possible that Network users may obtain keys related to child pornography images or videos directly from other Network users.

Investigation into the Trafficking of Child Pornography on the Network:

For some time now, law enforcement has been investigating the trafficking of child pornography on the Network. A modified version of the Network software is available to sworn law enforcement officers to assist in

conducting Network investigations. This law enforcement version is nearly identical to Network software, except that it allows a computer operated by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers.

Law enforcement computers do not target specific peers on the Network nor do law enforcement computers solicit requests from any peers. Network information collected by law enforcement computers is logged and provided to other trained law enforcement personnel in order to further investigations into Network users believed to be downloading child pornography files via the Network.

Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on the Network. Law enforcement only investigates Network users who request pieces of files associated with such keys collected by law enforcement. The keys collected by law enforcement have been obtained via publicly accessible sites, such as Network message boards and websites, as well as during the course of prior investigations into child pornography trafficking on the Network.

By viewing the documented activity of a peer that sends a request to a law enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of

a file of interest. A mathematical formula is applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer.

Requests Targeted in the Instant Investigation:

State Bureau of Investigation (SBI) Criminal Specialist (CS) Rodney White reviewed information obtained and logged by law enforcement Network computers related to IP address 174.111.32.203. In January and March 2018, the user requested pieces of child pornography files. Considering the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had – the number of requests for file pieces is significantly more than one would expect to see if the user were merely routing the request of another user. Accordingly, it is more likely than not that the user was the original requestor of the files.

Identification of Timothy Donovan BURNS as a Suspect:

Records obtained from Charter Communications revealed that IP address 174.111.32.203 resolved to "Don BURNS" at his apartment in Kernersville, North Carolina.

Seizure of Electronics & First Interview of BURNS:

On March 14, 2018, CS White and Homeland Security Investigations

(HSI) Special Agent (SA) Charles Cook traveled to BURNS's apartment to speak with him. BURNS answered the door and agreed to speak with the agents inside. Upon entry, the agents observed a desktop computer in the living room connected to a bay of hard drives. BURNS explained that he lived alone and was unemployed, though he formerly worked as a computer programmer.

When asked if he was familiar with file sharing programs, BURNS said that he was. He explained that he used the BitTorrent peer-to-peer network[2] years ago but stopped because law enforcement monitored it and would show up at people's homes. BURNS also stated that he had used Tor[3] in the past but didn't like it. When the agents informed him that they were working on a case involving the Network, BURNS admitted to using the Network.

CS White explained why the agents were present; specifically, that an individual using BURNS's IP address requested child pornography via the Network. When asked how long he had been using the Network, BURNS stated that he had been using it for a few months. BURNS stated that there was no

[2] Unlike the Network, anonymity is not a feature of the BitTorrent network.
[3] Tor is an online network that obfuscates a user's IP address thereby providing anonymity to online activities. United States v. McLamb, 880 F.3d 685, 688 (4th 2018). Hidden websites, or "services," are also available through the use of Tor. Id.

new child pornography on the Internet. He explained that it was all old stuff that he had already seen.

CS White asked BURNS what kind of child pornography files he had downloaded. BURNS replied that the agents should already know since they were monitoring his downloads. When asked what he did with the child pornography files, BURNS explained that he downloaded the files to a hard drive and then sorted through them, deleting the files he didn't want. BURNS said that he preferred minor girls 15 to 16 years of age. He further specified, the "jailbait" type pictures.

When asked if he had ever taken pictures of a minor female, BURNS said that he had never taken a nude picture of a minor girl. When asked if he had ever had sexual contact with a minor, BURNS said that he has never done anything like that with a child. BURNS also stated that the child pornography was for his personal use and that he did not upload, trade, or sell the images.

BURNS denied using any type of encryption software to protect his files. BURNS gave CS White verbal consent to take his computer and hard drives and examine them for child pornography. CS White asked BURNS which hard drive he used to save the child pornography that he downloaded. In response, BURNS explained that there were three hard drives connected to his desktop computer. The first contained the computer's operating system, the second was

the location to which files were downloaded, and the third contained music.

During the interview with the agents, BURNS sometimes qualified his answers by stating "If I was doing it…." and "….I'm not saying I did it" and then smiling.

BURNS executed a written consent permitting CS White to search his devices. With BURNS's permission, CS White took custody of the computer and hard drives.

Forensic Analysis of Electronic Devices:

CS White forensically examined BURNS's three computer hard drives. The first, a 250GB Crucial, was in fact the computer's operating system and contained deleted child pornography files, the second, a 2TB Hitachi, was fully encrypted by VeraCrypt software, and the third did in fact contain music files. SA White's analysis did not reveal any encrypted containers on the first or third drives.

The first hard drive, the operating system, contained 36 child pornography images that CS White recovered from unallocated space (i.e. they had been deleted from the active disk space). In the hard drive's active space, at the file path "user\WSPD Fraud\Desktop," CS White observed instructions on how to setup the Network and Tor on a full disk encrypted hard drive to prevent data leaks. The instructions were in the form of three images and

included how to use VeraCrypt software. CS White also located VeraCrypt software and the Tor browser on the hard drive's active space.

The Crucial hard drive possessed by BURNS was first available for purchase in February 2015.

Second Interview of BURNS:

On March 20, 2018, the agents returned to BURNS's residence to speak with him. BURNS again agreed to speak with the agents inside. CS White explained that the agents had returned to discuss the encrypted hard drive connected to his computer. When asked for the password to the hard drive, BURNS stated that the agents already knew what was on the drive. BURNS questioned why the agents needed to see the files that were on the hard drive. BURNS unequivocally stated that there was child pornography on the hard drive, but declined to provide the password because, as he put it, letting the agents see the files would not be in his best interest. BURNS said that the files on the hard drive were files that agents had seen in the past. BURNS again proclaimed that there was no new child pornography to be downloaded and that everything was old.

The agents advised BURNS that they wanted to access the files so that they could submit them to the National Center for Missing and Exploited Children (NCMEC) to determine if the children depicted had been identified.

BURNS stated that the agents had seen the files he had been downloading and thus, they should have the same files. CS White explained that the agents did not know *every* file that BURNS downloaded.

BURNS explained that the files he downloaded went to the default download folder and stayed there until he had time to look through them. BURNS again explained that he liked to download "jailbait" files and preferred girls between 15 and 16 years of age. CS White asked BURNS why he was reluctant to provide the password given that BURNS had admitted to downloading and possessing child pornography. BURNS again stated that it wasn't in his best interest to enable the agents to see the images stored on his hard drive.

Before the agents left, BURNS asked them to notify him before they came to arrest him.

This the 5th day of February, 2019.

Respectfully submitted,

MATTHEW G.T. MARTIN
United States Attorney

/S/ ERIC L. IVERSON
Assistant United States Attorney
NCSB #46703
United States Attorney's Office
Middle District of North Carolina
101 South Edgeworth Street
Greensboro, NC 27401
Phone: 336/332-6302

IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA	:	
	:	
v.	:	1:18CR492-1
	:	
TIMOTHY DONOVAN BURNS	:	

CERTIFICATE OF SERVICE

I hereby certify that on February 5, 2019, the foregoing was electronically filed with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the following:

Dylan Greenwood, Esq.

Respectfully submitted,

/s/ ERIC L. IVERSON
ASSISTANT UNITED STATES ATTORNEY
North Carolina State Bar No. 46703
United States Attorney's Office
Middle District of North Carolina
101 S. Edgeworth Street, 4th Floor
Greensboro, North Carolina 27401
Phone: (336) 333-5351
E-mail: eric.iverson@usdoj.gov